

Enhancing Software Defined Radio (SDR) security using variations in Gray Coded Mapping Scheme in Rectangular QAM

Saad Islam, Muhammad Ali, Umair Nasir, Fatima Ajmal, Salman Ali and Adnan Rashdi
Military College of Signals
National University of Sciences and Technology, Pakistan
saadislam, ali_siddiqi, umairnk, fatima, salmanali, adnanrashdi@ieee.org

Abstract - Secure communication includes means by which people can share information with varying degrees of certainty that third party cannot know what was said. This paper proposes a novel method for adding security in digital communication system through variations in gray coded mapping scheme in typical rectangular QAM. This will be achieved by varying the constellation mappings where by each symbol will be mapped to a different amplitude and phase level in a constellation plot at each variation (hop) without breaking the rules of gray coding i.e. only a single bit difference between adjacent symbols is maintained. The main focus will be on reconfigurable software defined radio (SDR) because the reconfiguration of mappings is very difficult to be achieved in hardware. It will be shown that there exist numerous mapping schemes similar in function to Gray coded mapping scheme. An important fact is that the application of security does not cause undesirable effects. That is to say that the Bit Error Rate (BER) vs. Signal to Noise Ratio (SNR) curves are not deteriorated and remain constant for each variation as explained in Section V.

Secondly the use of Bandwidth also stays constant unlike the Frequency Hopping Spread Spectrum (FHSS) technique where the security is achieved at the expense of increased bandwidth [1]. In addition further security can be achieved if these mapping schemes are varied pseudo randomly after a specified period of time. The ideas of hopping period and the number of hopping frequencies as used in FHSS can also be applied in the proposed method with a little alteration in the terminology. For example the time interval during which the communication system will work on any one of possible mapping schemes is still termed as hopping period, however we are not dealing with hopping frequencies here, instead we are hopping between various constellation mappings. It remains obvious that the shorter the hopping period and the higher the number of hopped mappings, the more secure is the communication system.

Keywords— SDR, QAM, Gray Code, Constellation Mapping

I. INTRODUCTION

Security is a major issue in communication systems. In telecommunications, the term **security** has the following meanings [2]:

“A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences.”

With respect to classified matter, the condition that prevents unauthorized persons from having access to official

information that is safeguarded in the interests of national security.

The threat to the privacy of the digital communication system have always persisted in the form of jammers, hackers and intruders incessantly exploiting the techniques used in the communication system for their own benefits. At the same time there do exist a number of ways in the communication system to counter them. Most commonly used are frequency hopping spread spectrum (FHSS) techniques, Cryptography, Steganography etc.

A **Software Defined Radio** (SDR) system is a radio communication system where components that have typically been implemented in hardware, for example mixers, filters, amplifiers, modulators/demodulators, detectors etc, are instead implemented using a software program on a personal computer or other embedded computing devices such as DSP and FPGA. The term "Software Defined Radio" was coined by Joseph Mitola in 1991, who published the first paper on the topic in 1992 [3]. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics are making many processes practical that were once only theoretically possible.

To be able to test the various modulation mapping schemes, reconfigurability is an important aspect in digital communication system. Hard-Wired implementation of our radio will not be helpful, as changing the mapping schemes will become impossible. However when the radio is software based i.e. SDR, the task of changing the mapping schemes becomes very simple.

In Section II we will discuss common modulation techniques in wireless communication standards and QAM. Section III will throw some light on rectangular QAM Modulation. In Section IV we will discuss various variations in Gray coded schemes. In Section V our proposed scheme is discussed. Finally the last part is devoted for conclusions.

II. QUADRATURE AMPLITUDE MODULATION

Modulation is the process of conveying the information over the medium. Digital modulation represents the transfer of the digital bit stream from the transmitter to the receiver(s) via the analogue informational channel (the medium).

During the modulation process the informational signal modifies one or more carrier parameters. Usually, the carrier is a sine wave, defined by amplitude, frequency and phase. Depending on the carrier parameter being changed, there are three basic types of modulation techniques:

- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)

In ASK the amplitude of the sinusoidal carrier is varied and in PSK the phase of the sinusoidal carrier is varied in correspondence to the signal being transmitted. If both amplitude and phase of the sinusoid are varied then the resulting modulation scheme is called QAM.

III. RECTANGULAR QAM

A QAM signal employs two quadrature carriers, $\cos 2\pi f_c t$ and $\sin 2\pi f_c t$, each of which is modulated by an independent sequence of information bits. The transmitted signal waveforms have the form [4]

$$u_m(t) = A_{mc} g_T(t) \cos 2\pi f_c t + A_{ms} g_T(t) \sin 2\pi f_c t \quad (1)$$

where A_{mc} and A_{ms} are the sets of amplitude levels that are obtained by mapping k -bit sequences into signal amplitude. For example, Fig.1 illustrates a 16-QAM signal constellation that is obtained by amplitude modulating each quadrature carrier by $M = 4$ PAM. M refers to the number of constellation points.

In general, rectangular signal constellations result when two quadrature carriers are each modulated by PAM.

Rectangular QAM constellations are, in general, sub-optimal in the sense that they do not maximally space the constellation points for a given energy. The non-square constellations achieve marginally better bit-error rate (BER) but are harder to modulate and demodulate.

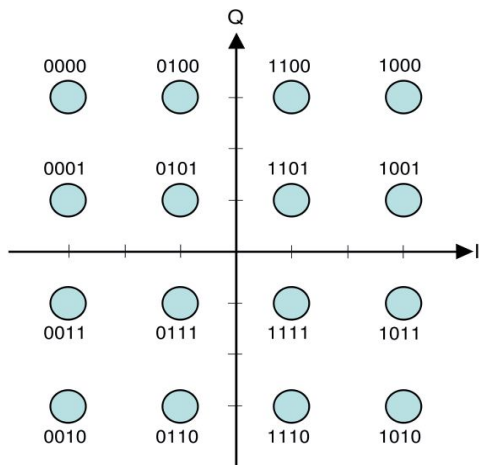


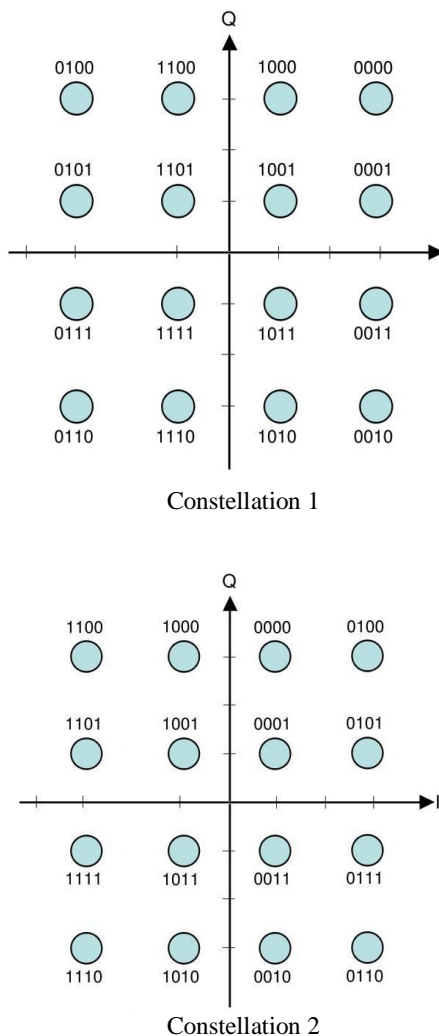
Fig. 1. Constellation diagram for rectangular 16-QAM

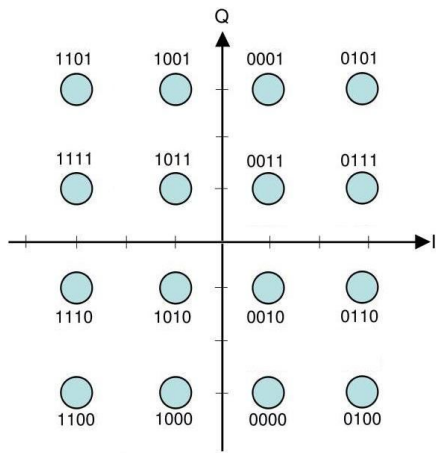
IV. GRAY CODE AND ITS VARIATIONS

The reflected binary code, also known as Gray code after Frank Gray, is a binary numeral system where two successive values differ in only one digit [5].

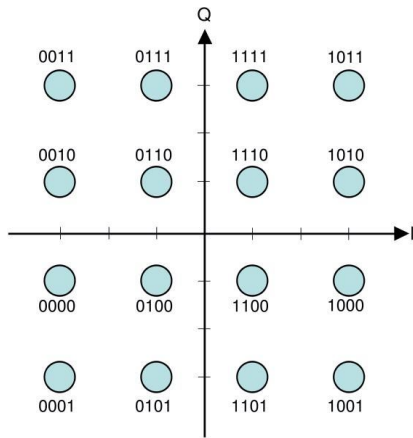
In modern digital communications, Gray codes play an important role in error correction. For example, in a digital modulation scheme such as QAM where data is typically transmitted in symbols of 4 bits or more, the signal's constellation diagram is arranged so that the bit patterns conveyed by adjacent constellation points differ by only one bit, as shown in Fig.1. By combining this with forward error correction capable of correcting single-bit errors, it is possible for a receiver to correct any transmission errors that cause a constellation point to deviate into the area of an adjacent point. This makes the transmission system less susceptible to noise effects.

But there are numerous other constellation arrangements in which the bit patterns of adjacent constellation points differ by only one bit, similar to Gray code. Some of the mappings are shown in Fig.2. These mappings can be referred to as constellation 1, 2, 3 and 4.





Constellation 3



Constellation 4

Fig. 2. Constellation arrangements other than Gray coded mapping for rectangular 16-QAM. Constellations 1 to 4.

V. PROPOSED METHOD

In the previous section variety of non-Gray coded constellation arrangements were shown which served the very purpose of a Gray coded arrangement. As shown in Fig.3 and Fig.4 the BER vs. SNR plots for each of the variations remain exactly the same as expected.

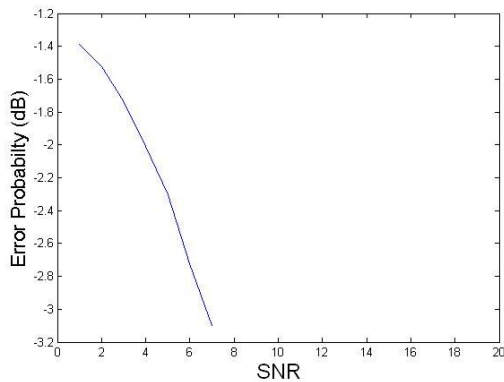


Fig.3 . BER vs. SNR plot for Gray coded 16-QAM Signal Constellation

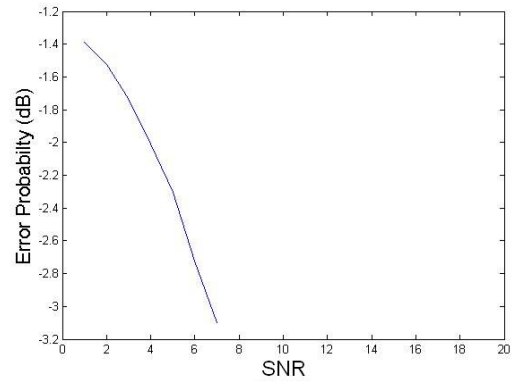


Fig. 4. BER vs. SNR plot of one of the variation in Gray coded mapping scheme

Now we come towards the idea presented in this paper. Recently, techniques have been developed to detect the modulation technique employed in an intercepted or an unknown received signal. Efficient blind demodulation detection algorithms exist that find the exact modulation technique employed in the received signal [6]. As the modulation detection techniques get better, this becomes a huge problem for organizations requiring secure communication.

If we somehow vary the constellation arrangement in a pseudorandom manner similar to FHSS, then the unauthorized receiver will be handed a difficult task of continuously detecting the exact arrangement. The detection job will become more difficult if we increase the hopping rate, eventually at some point it will become impossible.

A different signal mapping exists against each entry of pseudo-random sequence generator. Table.1 illustrates a typical scheme used for a group of 4 constellation arrangements of Fig.2 where a different mapping constellation is selected against each entry of the PN Sequence Generator.

PN Sequence Generator	Mapping
1	Constellation 1
2	Constellation 4
3	Constellation 2
4	Constellation 3

Table. 1. PN Sequence and the corresponding constellation

At the end of the sequence, the PN sequence generator is reset and Table 1 repeats itself. It is important to emphasize that greater number of constellation arrangements and lesser hop period would ensure increased security to the communication system.

Analysing Fig.2 and the Table.1, the bit sequence 0100 is mapped at different signal amplitudes in each constellation. Thus without knowing the exact sequence as in Table 1, the intruder has very little chance to demodulate data to exact bit sequence.

The next issue is the generation of these constellation arrangements at both the modulator and demodulator at transmitter and receiver respectively. In non-flexible hardware

radio, varying these constellation arrangements is out of question. So here we can employ the concept of SDR where the reconfigurability advantage helps us achieve our goal in an effective manner.

Fig.5 shows the essential blocks required in our proposed method for achieving added security in a digital communication system.

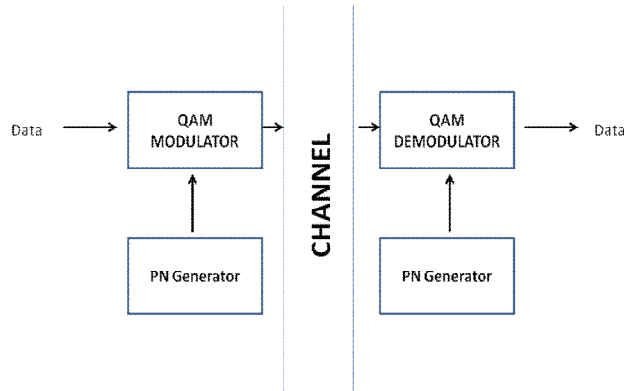


Fig. 5. Essential blocks to ensure variation in gray coded QAM signal constellation

VI. CONCLUSION

In section IV, a variety of non-Gray coded constellation arrangements were shown which served the very purpose of a Gray coded arrangement. If all the constellation arrangements which are continuously varied are those which abide by the function of Gray coded arrangement (as discussed in section IV), then the degradation of BER vs. SNR curves will not occur as all the curves will be exactly the same (as shown in Fig.3). Thus this technique can provide enough security to the digital communication system without any hardware complexity, increased error rate and bandwidth.

REFERENCES

- [1] Behrouz Forouzan, *Data Communications and Networking, Bandwidth Utilization: Multiplexing and Spreading: Spread Spectrum*, 4th Edition, Page 181.
- [2] *Federal Standard 1037C*. Institute for Telecommunications Sciences. Retrieved on 2007-10-14.
- [3] J. Mitola, "The Software Radio," *IEEE National Telesystems Conference*, 1992 - Digital Object Identifier 0.1109/NTC.1992.267870
- [4] J. Proakis and M. Salehi. (1998) *Contemporary Communication Systems Using MATLAB*. pp. 304-306
- [5] F. Gray. *Pulse code communication*, March 17, 1953 (filed Nov. 1947). U.S. Patent 2,632,058
- [6] Sharath B. Reddy, Tevfik Yucek and Huseyin Arslan, "An Efficient Blind Modulation Detection Algorithm for Adaptive OFDM Systems."